



HIPAA

A Look Inside

Why HIPAA?

The 104th Congress

Sought to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.



A National Effort to Standardize-- HIPAA!

The Health Insurance Portability and Accountability Act of 1996, Administrative Simplification, requires payers, providers, and claims clearinghouses to establish protections, adopt standards, and meet requirements for the transmission, storage, and handling of certain health care information.

HIPAA Exemptions Exist But May Have Long-Term Implications

- A provider of services with fewer than 25 full-time equivalent employees
- A physician, practitioner (pharmacy), facility, or supplier with fewer than 10 full-time equivalent employees
- No EDI



Overall Compliance... Aim For The “Bull’s Eye” Ongoing Efforts Likely To Continue

Transactions, Code Sets, Identifiers – October 16, 2003

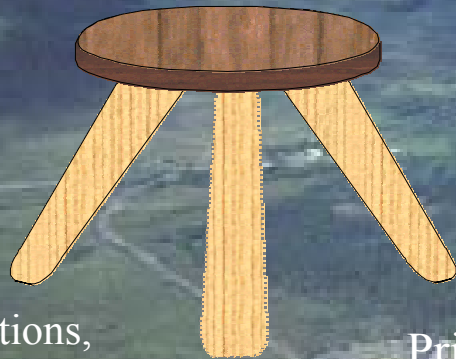
Privacy – April 14, 2003

Security – April 21, 2005

Our Discussion

Administrative Simplification

Future Regulations Pending



Transactions,
Code Sets,
Identifiers

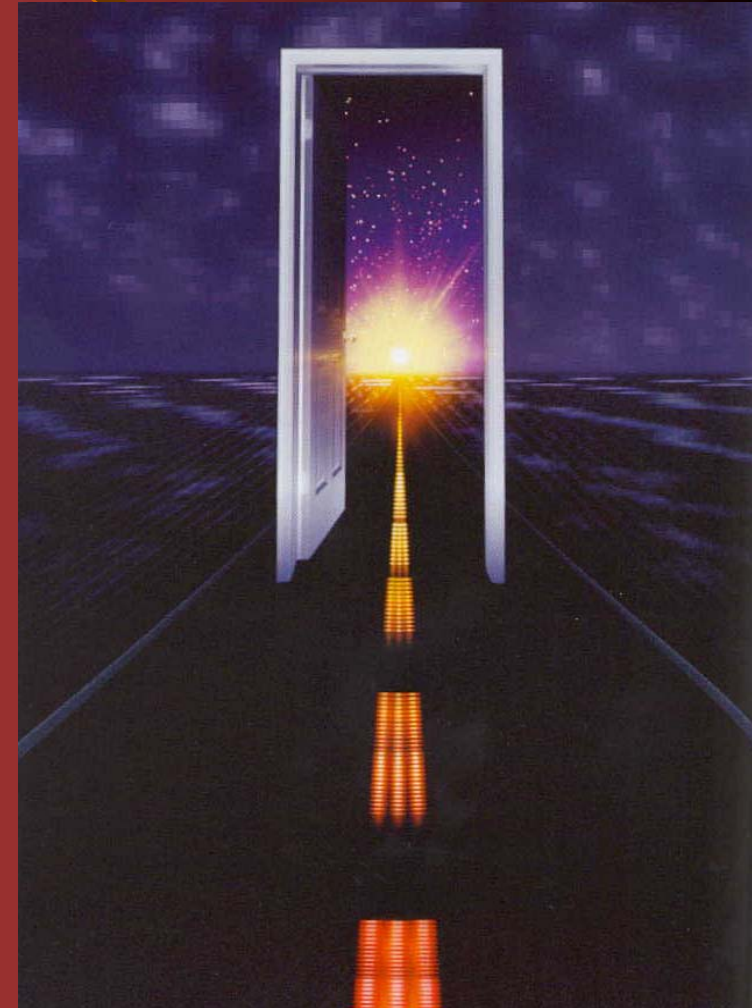
Security

Privacy

HIPAA

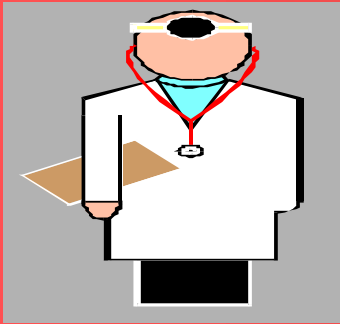
Expected To Evolve Over Time...

- The Secretary (HHS) may adopt a modification to a standard once a year
- The Secretary may adopt a modification at any time during the first year after the standard is adopted
 - Compliance date can be as early as 180 days after modification is adopted
 - Small health plan compliance date can be extended



HIPAA

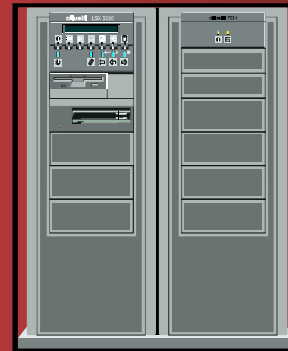
Scalable To All Covered Entities...



Health
Care Providers



Hospitals



Claims
Clearinghouses



Payers

Think "reasonable" when deciding on implementation activities

HIPAA Enforcement

“A Carrot And Not A Stick”

- Robin Frohboese, Principal Deputy & Acting Director of the Office for Civil Rights has stated that identified violations are viewed as an opportunity to educate covered entities back into compliance.
 - “It’s critically important that covered entities understand their responsibilities and that we help them with compliance so our enforcement is minimized. If we find violations, we will seek voluntary compliance. It will only be in the most egregious situations where we are not able to get voluntary compliance that we will do other things, such as civil monetary penalties or, in the worst situations, refer to the Justice Department.”

Source: Report on Patient Privacy, May 2002

Accountability

- *Civil penalties* against a covered entity that fails to comply
 - \$100 per incident
 - Up to \$25,000 per person/year/standard violated
 - Enforcement by HHS Office for Civil Rights
- *Federal criminal* penalties for knowingly and improperly disclosing or obtaining protected health information
 - Up to \$250,000 and up to 10 years in prison
 - Enforcement by Department of Justice

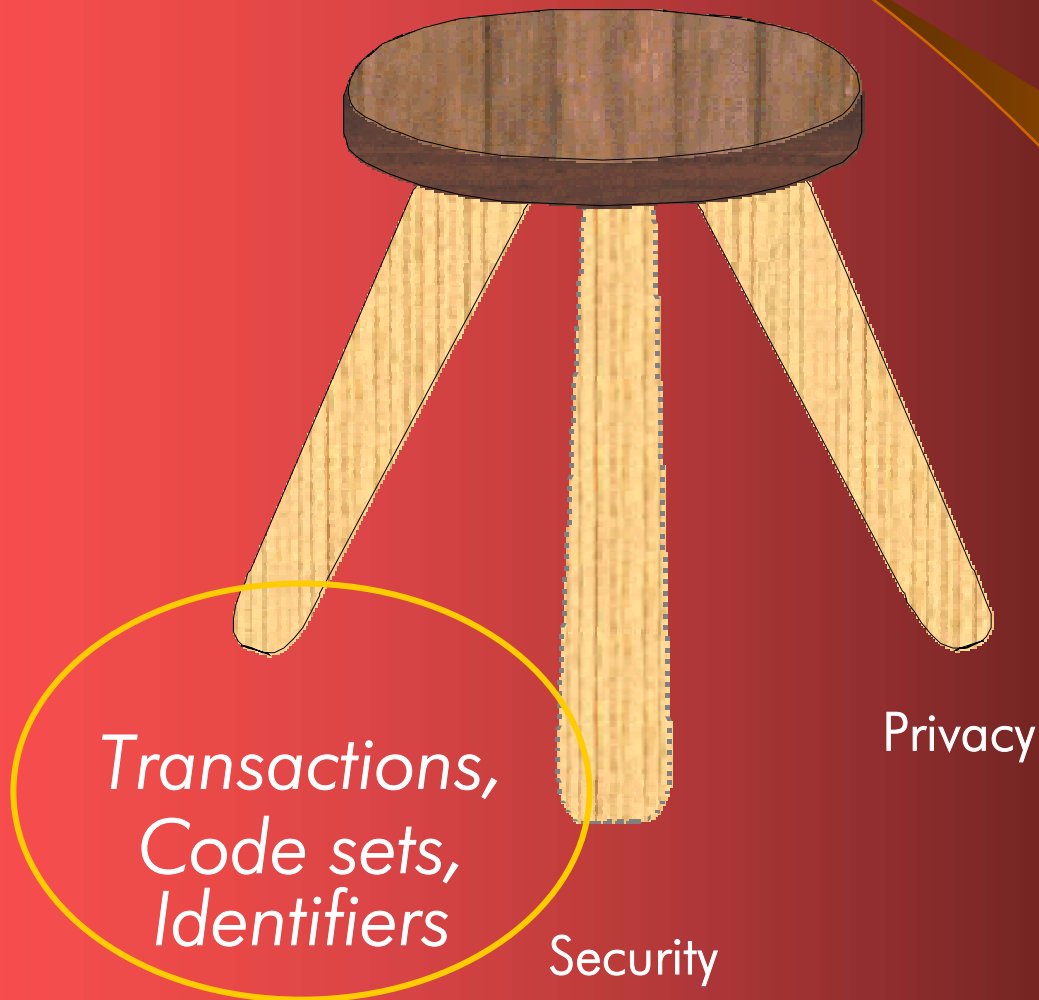


Compliance Monitoring

- Centers for Medicare and Medicaid Services (CMS) monitors compliance on the transaction and code set standards
- The Office for Civil Rights will monitor compliance on the privacy and security regulations
- Audits can be unannounced
- Keep compliance activities in perspective

HIPAA

Transactions & Code Sets



HIPAA Transactions

Standardize Health Information

- Payers and electronic health networks must be capable of electronically accepting:
 - Enrollment in a health plan,
 - Eligibility for a health plan,
 - Health claims (retail drug, dental, professional, and institutional)
 - Health care payment & remittance advice
 - Health plan premium payments,
 - Health claim status,
 - Referral certification, authorization, coordination of benefits (Rx: NCPDP Telecommunication Guide)

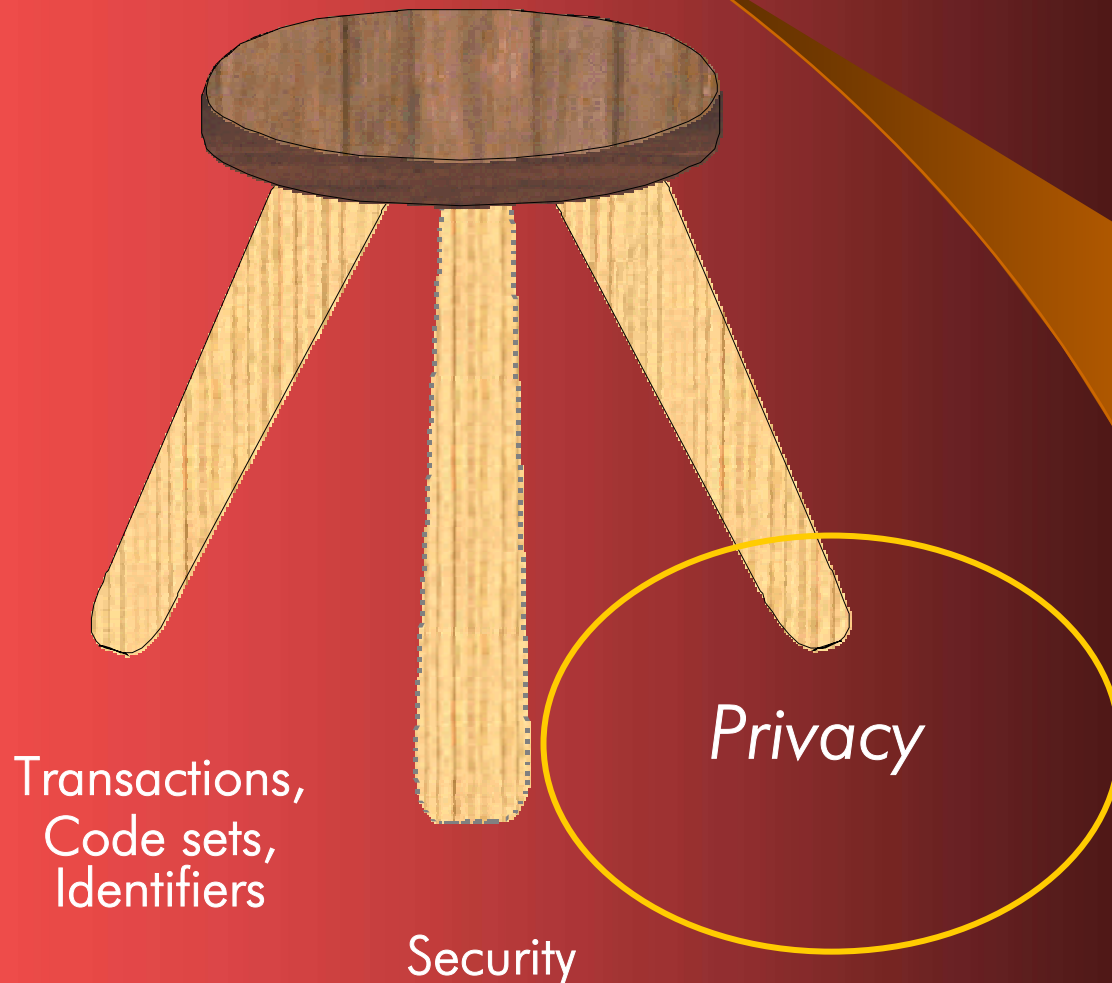
Transaction Testing Certification Vendors

- Claredi – www.claredi.com
- EDIFECs – www.edifecs.com
- Foresight Corporation – www.foresight.com
- GFEGUSA – www.gfeg.com
- AppLabs, Inc. – www.applabs.com

HIPAA Transactions.... **You Manage The Process**



HIPAA Privacy



Why Do We Need Privacy Regulations?



Mary – our car insurance is up. Seems you have a 24% chance of developing narcolepsy based on your father having diabetes.

Steven—you are to begin therapy, as your blood test indicates 25% risk of teenage depression based on your genetic profile.

Father just got a telemarketing call from a home blood sugar monitoring service. But I don't think he ever followed up on that office visit to the doctor!

HIPAA

Privacy Regulations

- *Protected Health Care Information (PHI) is defined as:*

Individually identifiable health care information created or received by a provider, payer, or claims clearinghouse related to health condition, provision of health care, or payment for health care

The final rule was extended in scope to include the protection of all individually health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity. This includes PHI in paper records that never have been electronically stored or transmitted

Protected Health Information (PHI)

The 19 Identifiers

- Name
- Address
- E-mail
- Dates
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate Number
- License Number
- Vehicle Identifiers
- Facial Photographs
- Telephone Numbers
- Device Identifiers
- URLs
- IP Addresses
- Biometric Identifiers
- Geographic Units
- Any Other Unique Identifier Or Codes

Provider Discretion

- *Did you know that...*

“A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual’s best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protect health care information.”

- Page 44 (3) Limited uses and disclosures when the individual is not present, 2nd sentence of the Final Privacy Rule – Regulation Text



Permitted Uses & Disclosures Research

- A covered entity may use or disclose protected health care information for research, regardless of the source of funding of the research provided that approval is obtained by a:
 - Privacy Board
 - Institutional Review Board
- Limited data set allows use of PHI providing 16 identifiers are removed and a Data Usage Agreement is signed. A limited data set excludes specific, readily identifiable information

Uses and Disclosures – Marketing and Fundraising

- Must obtain an individual's prior written authorization for marketing purposes except:
 - Face-to-face
 - Products of minimal value
 - Concerns health-related products judged beneficial
 - Communication involving a promotional gift
 - *Must take steps to allow opt out*
- May disclose to fundraising arm without authorization
 - Dates of care, limited demographic data
 - Must provide opportunity to opt out

Minimum Necessary Concept

- When using or disclosing reasonable efforts must be made to limit PHI to that necessary to accomplish the intended purpose
- Applies to discloser and requestor
 - *Uses:*
 - Role based access
 - Need to identify types of workers, types of information, and condition of access
 - *Disclosures:*
 - Routine disclosures
 - Non-routine disclosures
- *Does not apply to disclosure to providers for treatment*

Confidential Communications

- A covered entity must permit an individual to request, and it must accommodate reasonable requests to receive communications of PHI by provider by alternative means and location
 - Some examples: E-mail, pager, voice mail, friends/relatives home, other possibilities



Consent - Optional

- A consent allows a provider to use or disclose protected health care information to carry out treatment, payment, & health care operations
- One time only:
 - Inform that protected health information may be used or disclosed for treatment, payment, or health care operations
 - Refer to notice of privacy practices
 - State the right to request restrictions
- May condition treatment based on consent
- May be revoked
- Provider must document & retain consent forms
- Attempts to obtain a consent must be documented

Authorization

- Authorization is more detailed and specific than consent
 - Limited to only information to be disclosed
 - Recipient of information
 - Includes an expiration date
- Core elements of a valid authorization:
 - A description of the information to be used or disclosed
 - The name or other specific identification of the person authorized to make the requested uses and disclosures
 - An expiration date or expiration event
 - A statement of the individual's right to revoke the authorization in writing
 - A statement that information used or disclosed may be subject to re-disclosure by the recipient
 - Signature of the individual and date
- Authorizations must be written in plain language

Notice Of Privacy Practices – Things To Think About

- An individual has the right to adequate notice of the uses and disclosures of protected health care information
- The covered entity must provide a notice that is written in plain language
- Direct treatment providers to make a good faith effort to obtain a patient's written acknowledgement of the notice
- In emergency situations, the notice must be provided as soon as is reasonably practical
- Notice can be mailed

Notice Of Privacy Practices - Elements

- Notice can be layered with summary information at the top and more detailed information at the bottom
 - *Header:* This notice described how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully. Clarification of an individuals privacy rights
 - *A description and at least one example* of the types of uses and disclosures
 - *A description of each of the purposes* for which the covered entity is permitted or required to disclose PHI

Notice Of Privacy Practices - Elements

(Continued)

- *A statement that uses and disclosures* follow more stringent State or Federal laws
- *A statement that other uses and disclosures* will be made only with the individuals written authorization and that the individual may revoke such authorization
- *Separate statements for certain* uses or disclosures
- *Complaint contact*
- *Contact name* for obtaining other information
- *Effective date*

Notice Of Privacy Practices - Elements

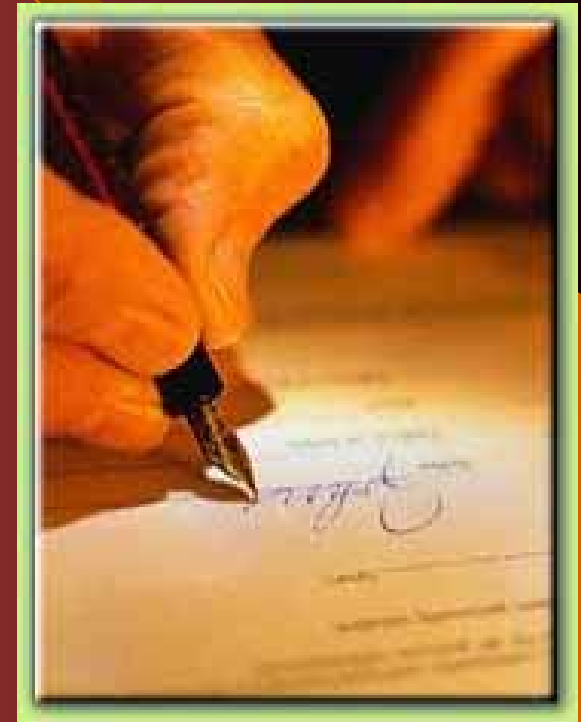
(Continued)

- *Revision practice* and distribution process
- *Providers must provide* on the first date of service
- *Notice must be available on site* for distribution and prominently posted
- *A notice must be maintained on a covered entity's Web site* that provides customer service or benefit information

Business Associate Contract

An Agreement Between Parties

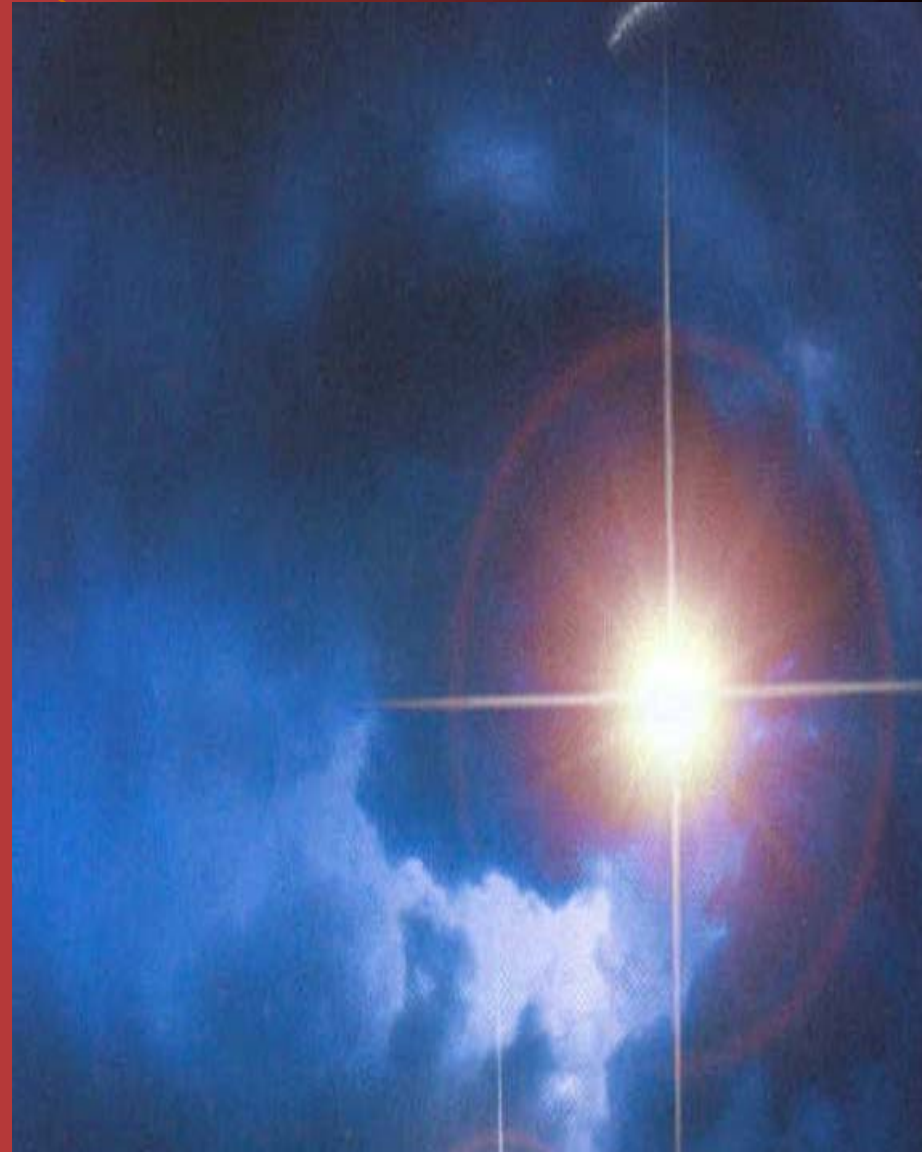
- Acts on behalf of a covered entity in conducting activities involving use of PHI
- Covered entities are not responsible for actions of business associates
- Monitoring is not required
- An organization can be both a covered entity and a business associate
- Due April 04



Business Associate Contract

(Continued)

- Limit contents to information specific to PHI
- Trading partners will be reluctant to sign complex Business Associate Contracts
- Trading partners are less likely to incur legal fees on easy to read Business Associate Contracts
- Keep it simple



Individual Access To PHI

- Must permit access within 30 days of the request
 - One 30 day extension is permissible
- Ordinary access for as long as information is maintained
 - Practitioner discretion relating to psychiatric notes
 - Information compiled as part of a civil, criminal, or administrative action is exempted
- Unreviewable grounds for denial
 - Research

Individual Access To PHI

(Continued)

- Information was obtained by someone other than the health care provider under a promise of confidentiality
- Reviewable grounds for denial
 - In some circumstances a request can be reviewed by another licensed professional
 - Usually relates to professional judgment

Patient Awareness Of New HIPAA Rights - Not Too Far Off...

- Right to inspect and copy protected health information
- Right to amend
- All approve uses and disclosures
- Right to an accounting of disclosures
- Right to have reasonable requests for confidential communication accommodated
- Right to file a written complaint
- Right to receive written notice of information practices

Some Leading HIPAA Myths



Protecting Patient Information What's Really Required?

The regulations do not describe the particular measures a

covered entity must take to meet the standard, variation is likely

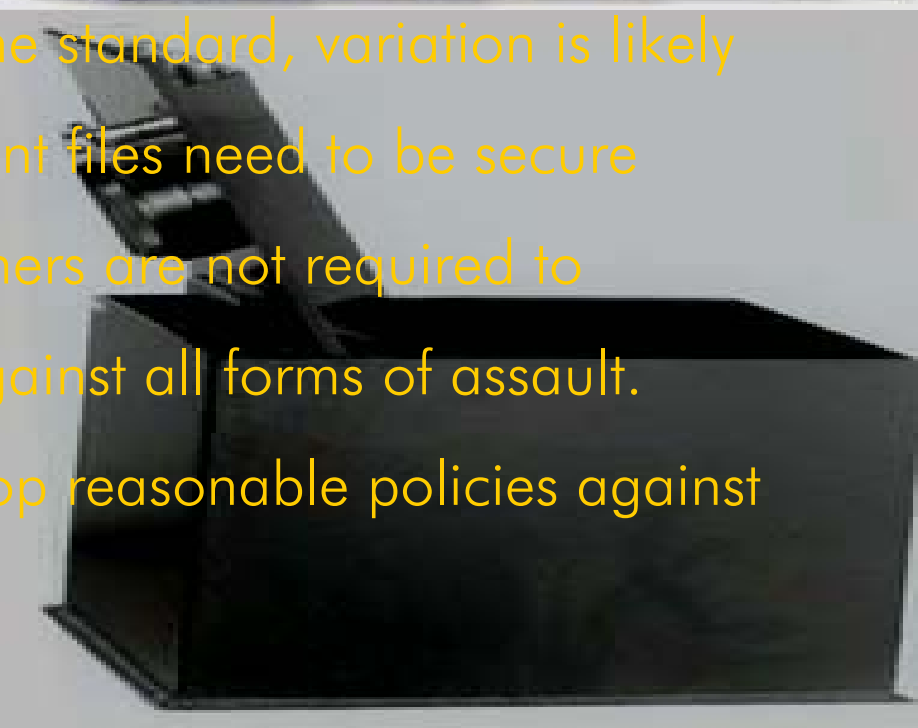
to exist among practitioners. Patient files need to be secure

within a secure location. Practitioners are not required to

guarantee the protection of PHI against all forms of assault.

Practitioners are required to develop reasonable policies against

theft of PHI.



What About Signature Logs & Sign In Sheets

- HIPAA does not require providers to use tracking sheets
- Consider its purpose and value
- Look for opportunities to limit potential disclosure of PHI
- *Evaluate low cost alternatives*



Shredders – Their Value To Providers



Protecting Anonymity In Waiting Rooms--- Is This Possible?



Administrative Requirements

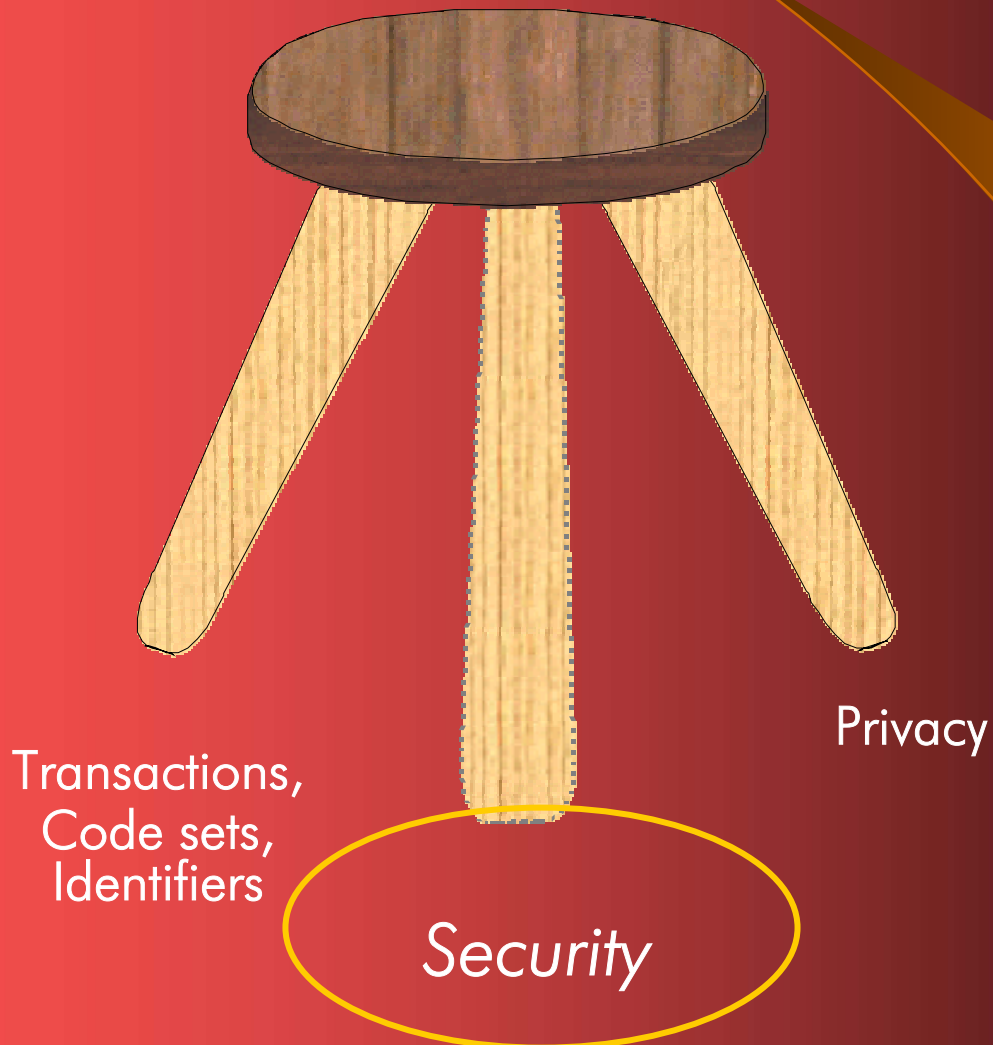
- Implementation allows for flexibility and scalability
 - Response can be geared to your environment
- Covered entities are required to:
 - Designate a privacy official
 - Develop policies and procedures
 - Notices of practices
 - Provide privacy training to its workforce
 - Develop a system of sanctions for employees who violate the entity's policies
 - Meet documentation requirements

Administrative Requirements (Continued)

- A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law
- When a covered entity changes a privacy practice that is stated in the notice, it may make the change effective for PHI that was created or received prior to the date of the notice providing the notice reserves the right to make such change in its privacy practices
- A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented

HIPAA

Security “Proposed”



HIPAA Security Standards An Overview

Three Security Categories:

- Administrative Safeguards

Development and implementation of security measures to protect data and the conduct of personnel in relations to the protection of data

- Physical Safeguards

The protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as intrusion

HIPAA Security Standards

An Overview (Continued)

- Technical Safeguards

The process that's put into place to protect information and to control and monitor individual access to information

Security Elements - Detail

Administrative Safeguards:

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

Security Elements – Detail (Continued)

Physical Safeguards:

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Security Elements – Detail (Continued)

Technical Safeguards:

- Access control
- Audit control
- Integrity
- Person or Entity Authentication
- Transmission Security

HIPAA Privacy Preparing Your Organization For Compliance...



HIPAA

Sound Documentation Is Essential

- Transaction Standards & Code Sets
- Privacy
- Security



Policies and Procedures

Preparing Your HIPAA Compliance Manual

- Transaction Standards
 - *Vendor self-certification letter or third party certification (include specific transactions)*
- Privacy
 - *Gap assessment: Q&A*
 - *Policies and procedures*
 - *Sample forms*
 - *Training log*
- Security
 - *Gap assessment: Q&A*
 - *Policies and procedures*
 - *Sample forms*
 - *Training log*
- Ongoing review of your compliance manual is required

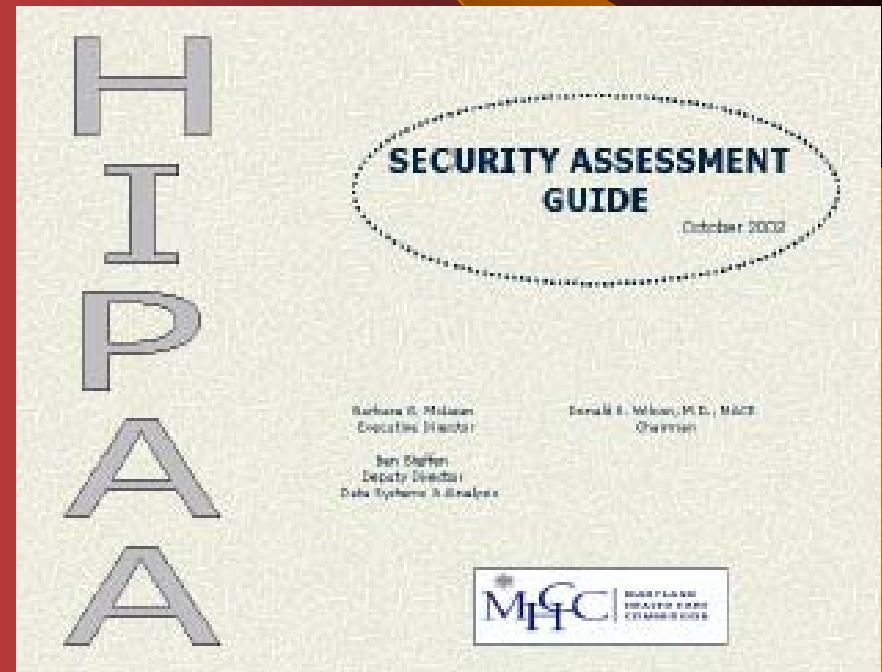
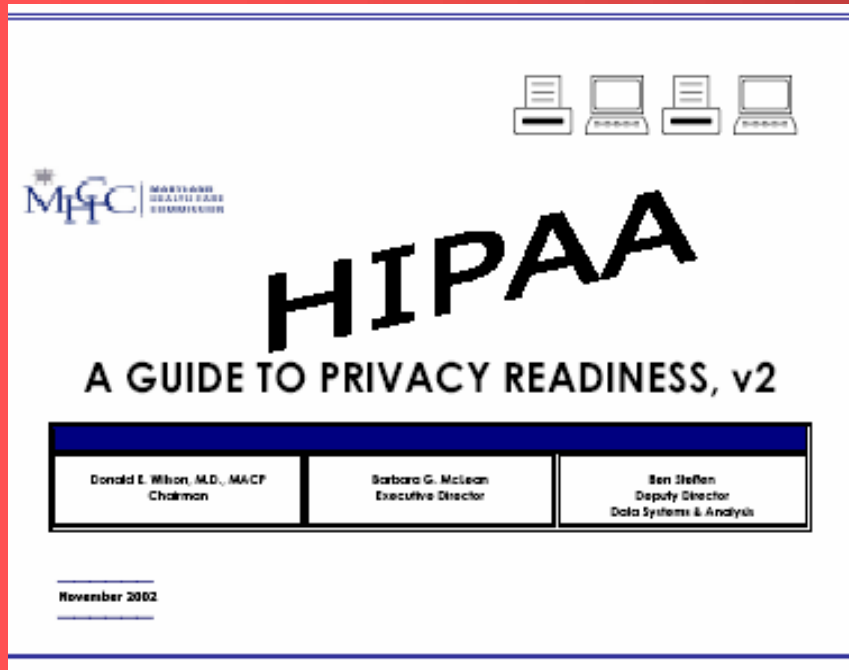
Policies And Procedures Updates & Deletions

- Practitioners must keep policies and procedures current to comply with changes in the law, standards, and requirements
- Changes in policies and procedures are only effective from that point in time forward
- Practitioners can make policy and procedure changes at any time
- Must be reviewed by all workforce during training

HIPAA Assistance For Providers

- An easy to use gap assessment tool for providers:

Both are available at the MHCC Web-site



Privacy Readiness Assessment Guide


“A Real Help To Providers”

- The EDI/HIPAA Workgroup decided on eight sections:
 - Introduction
 - Maryland Law on the Confidentiality of Medical Records
 - HIPAA Definitions
 - Assessment Guide and Work Plan
 - Business Associate Contract (illustrative document)
 - Chain of Trust Partner Agreement (illustrative document)
 - Notice of Privacy Practices (illustrative document)
 - Computer and Information Usage Agreement (illustrative document)

Security Readiness Assessment Guide

- The EDI/HIPAA Workgroup decided on eight sections:
 - Introduction
 - Definitions
 - Small Provider Implementation Example
 - Assessment Guide and Work Plan
 - Administrative Procedure Checklist
 - Physical Safeguards Procedures Checklist
 - Technical Security Services Procedures Checklist
 - Technical Security Mechanisms Procedures Checklist

Imagine A Time Period When...

- 
- Patients only schedule medical services, buy products, and use pharmacies that are HIPAA compliant
 - Liability carriers insure based upon HIPAA compliance
 - Financial institutions underwrite loans/lines of credit based upon HIPAA compliance
 - Payers require electronic transactions

Lasting Thoughts....

- Other final rules expected to be released
- Ongoing modifications of existing rules likely to occur
- Continue to become “HIPAA Wise”
- Implementation dates are “start dates” not “end dates”

For More Information on HIPAA

Official Sites

Government sites:

<http://aspe.hhs.gov/admnsimp> - Department of Health and Human Services

<http://www.hcfa.gov/security/iseclplcy.htm> - HCFA Internet Security Policy

<http://www.wpc-wdi.com/hipaa> -- Implementation Guides

Non-govt sites:

<http://www.wedi.org>

<http://www.nchica.org>

<http://www.hipaadvisory.com/>

MHCC site:

<http://www.mhcc.state.md.us>



